AUSGABE 05
MAI 2024

THOUVENIN
WEKA

DATENSCHUTZ

FÜR SCHWEIZER UNTERNEHMEN UND INSTITUTIONEN

DATENSCHUTZ AKTUELL

Haftet die Datenschutzberaterin für alle Verstösse?

Mehr dazu auf Seite 3

DATENSCHUTZ IM ARBEITSVERHÄLTNIS

Unterzeichnung der Datenschutzerklärung – Ist das wirklich notwendig?

Mehr dazu auf Seite 5

DATENSCHUTZ UND IT

Das Datenschutzgesetz gilt nicht für den B2B-Bereich – trifft das zu?

Mehr dazu auf Seite 7

DATENSCHUTZ AUS DER PRAXIS

«Betroffene Personen haben nur das Recht auf Auskunft, mehr nicht»

Mehr dazu auf Seite 10

Editorial

Von Marco S. Meier, RA, MLaw, CIPP/E | Counsel bei THOUVENIN Rechtsanwälte KLG

LIEBE LESERIN, LIEBER LESER

Ich freue mich sehr, Sie zu dieser Ausgabe des WEKA-Newsletters «Datenschutz» zu begrüssen.

Im Rahmen der Beratungstätigkeit stösst man immer wieder auf unterschiedliche Meinungen zu bestimmten datenschutzrechtlichen Pflichten. Das ist nicht unüblich, weil viele datenschutzrechtliche Herausforderungen noch nicht abschliessend geklärt sind. Darunter finden sich aber regelmässig Datenschutz-Mythen. Diese halten sich meist hartnäckig und erschweren die praktische Umsetzung der betreffenden gesetzlichen Pflicht, obwohl dies nicht zwingend notwendig wäre. In dieser Ausgabe widmen sich die Autoren solchen Mythen, entzaubern diese und zeigen praxisnah auf, wie damit umgegangen werden kann.

Ein Thema, um welches sich viele Mythen ranken, ist die Haftung der Datenschutzberaterin. Im Fokus steht neben der Frage, ob eine solche zwingend benannt werden muss, regelmässig die Frage nach der Haftbarkeit der Datenschutzberaterin, insbesondere welchen Haftungsrisiken sich die Datenschutzberater aussetzen. Auch im Rahmen des Mitarbeiterdatenschutzes bestehen zum Teil divergierende Auffassungen. Eine davon betrifft die Informationspflicht gegenüber den Mitarbeitenden in einer Datenschutzerklärung und die Frage, ob diese den Mitarbeitenden zur Unterzeichnung vorgelegt werden muss. Ferner stösst man in der Praxis auf die Behauptung, dass das Datenschutzrecht im Business-to-Business-Bereich nicht anwendbar sein soll. Doch stimmen diese Behauptungen mit den anwendbaren Rechtsnormen überein, oder handelt es sich tatsächlich um beharrlich verbreitete Mythen?

Diese Ausgabe des WEKA-Newsletters «Datenschutz» geht den vorangehend beschriebenen und weiteren Behauptungen nach. Die Autoren zeigen nicht nur auf, was es im konkreten Fall mit der Behauptung auf sich hat, sondern sie präsentieren konkrete, praxistaugliche Ansätze zum Umgang mit solchen Mythen:

Der erste Beitrag von Eleonor Gyr **«Haftet die Datenschutzberaterin für alle Verstösse gegen das DSG?»** beschäftigt sich mit dem wichtigen Thema der Haftung der Datenschutzberaterin.

Im zweiten Beitrag **«Unterzeichnung der Datenschutzerklärung durch Mitarbeitende – ist das wirklich notwendig?»** gehen Anna Neukom Chaney und ich der Frage nach, ob eine Datenschutzerklärung von Mitarbeitenden gegengezeichnet werden muss oder nicht.

Der Beitrag **«Das Datenschutzgesetz gilt nicht für den B2B-Bereich – trifft das zu?»** von Dirk Spacek stellt sich dem Mythos, der Anwendung des DSG im Bereich Business-to-Business.

Abschliessend beleuchtet der Beitrag **«Betroffene Personen haben nur das Recht auf Auskunft, mehr nicht – stimmt das denn wirklich?»** von Alesch Staehelin, ob den betroffenen Personen neben dem Auskunftsrecht auch weitere Rechte zustehen.

Ich wünsche Ihnen eine aufschlussreiche, spannende Lektüre.

Marco S. Meier, RA, MLaw, CIPP/E
Herausgeber

DER HERAUSGEBER

Marco S. Meier ist Counsel bei der Anwaltskanzlei THOUVENIN Rechtsanwälte KLG und ist spezialisiert auf Informations- und Kommunikationstechnologierecht (ICT). Er berät und vertritt seine Klienten in sämtlichen Bereichen des IT-, Datenschutz-, Cybersecurity- und Immaterialgüterrechts sowie in technologiebezogenen Compliance-Fragen. Als ausgebildeter Informatiker und Certified International Privacy Professional Europe (CIPP/E) hat er umfassende Erfahrung bei der Durchführung von Datenschutz-Compliance-Projekten, sowohl nach Schweizer Recht als auch nach der EU-Datenschutz-Grundverordnung, in Software- und Lizenzfragen sowie Technologie- und Outsourcing-Projekten in verschiedenen Branchen. Die Beilegung von Streitigkeiten im ICT-Bereich sowie die Beratung im Werberecht sind weitere Schwerpunkte seiner Tätigkeit.

www.thouvenin.com
m.meier@thouvenin.com

Haftet die Datenschutzberaterin für alle Verstösse gegen das DSG?

Mit Einführung des Datenschutzgesetzes (DSG) wurde auch in der Schweiz die Rolle der Datenschutzberaterin / des Datenschutzberaters eingeführt. Die Rolle kennen viele international tätige Unternehmen bereits von der europäischen Datenschutz-Grundverordnung (DSGVO), wobei sie dort Datenschutzbeauftragte genannt wird (meist abgekürzt DPO, das für Data Privacy Officer steht). In der Schweiz ist für Bundesorgane die Ernennung einer Datenschutzberaterin Pflicht, für private Verantwortliche hingegen nicht.

Von Eleonor Gyr

Aufgaben der Datenschutzberaterin

Die Datenschutzberaterin ist Anlaufstelle für betroffene Personen, wenn diese beispielsweise ihre Rechte (z. B. Auskunftsrecht) geltend machen wollen, aber auch für die Datenschutzbehörden resp. den Eidgenössischen Datenschutzbeauftragten (EDÖB).

Dem DSG können die folgenden Aufgabenfelder der Datenschutzberaterin entnommen werden:

1. Datenschutzschulung und -beratung
2. Mitwirkung bei der Anwendung der Datenschutzvorschriften

Eine Kernaufgabe der Datenschutzberaterin ist also die interne Schulung und Beratung des Unternehmens (oder Bundesorgan). Daher ist es unabdingbar, dass diese Person nicht noch andere Aufgaben innehat, die mit der Rolle als Datenschutzberaterin in einem Interessenkonflikt stehen (z. B. im Einkauf). Daneben ist die Mitwirkung beim datenschutzkonformen Handeln durch das Unternehmen (oder Bundesorgan) eine weitere essenzielle Aufgabe. Darunter fallen beispielsweise die Überprüfung von rechtskonformer Bearbeitung von Personendaten durch das Unternehmen (oder Bundesorgan), die Bearbeitung von Gesuchen von betroffenen Personen oder die Meldung, Aufarbeitung und Initiierung von Korrekturmassnahmen bei Datenschutzverletzungen. Das DSG spricht explizit von Mitwirkung und nicht von Sicherstellung datenschutzkonformen Handelns, da die Datenschutzberaterin in der Regel keine abschliessende Entscheidungskompetenz bezüglich datenschutzkonformen Handelns innehat, diese obliegt der Verantwortlichen (Geschäftsleitung oder Verwaltungsrat resp. entsprechendes Gremium in der Bundesbehörde).

Damit die Datenschutzberaterin ihre Aufgaben wahrnehmen kann, muss der Verantwortliche dieser Person auch die entsprechenden Mittel und Kompetenzen zur Verfügung stellen. Dies betrifft einerseits (finanzielle und/oder personelle) Ressourcen, um die obgenannten Aufgaben erfüllen zu können. Andererseits muss die

Datenschutzbeauftragte Zugang zu allen relevanten Informationen und Unterlagen haben, damit sie ihre Aufgaben auch tatsächlich wahrnehmen kann. Essenziell ist auch die Bestimmung, dass die Datenschutzberaterin die Kompetenz haben muss, in wichtigen Fällen das oberste Organ (Geschäftsleitung oder Verwaltungsrat resp. entsprechendes Gremium im Bundesorgan) zu benachrichtigen. Konkret bedeutet dies, dass die Datenschutzbeauftragte organisatorisch und hierarchisch unabhängig agieren können muss, typischerweise ist diese Person bei einem Unternehmen direkt dem CEO unterstellt und hat die Kompetenz, in wichtigen Fällen direkt den Verwaltungsrat zu kontaktieren. Die Rolle der Datenschutzberaterin ist also vergleichbar mit derjenigen eines Compliance Officers. Die Praxis zeigt, dass bezüglich der richtigen hierarchischen und organisatorischen Eingliederung in der Organisation bei vielen kleineren Unternehmen noch Nachholbedarf besteht.

Kompetenzen der Datenschutzberaterin

Damit die Datenschutzberaterin die obgenannten Aufgaben erfüllen kann, muss sie über die erforderlichen Fachkompetenzen verfügen. Es ist dabei nicht zwingend, dass diese Person eine juristische Ausbildung hat, wobei eine entsprechende Ausbildung sicherlich hilfreich ist. Oft werden die Fachkenntnisse in der Praxis mit entsprechenden Weiterbildungen und Zertifikaten belegt (z. B. CAS Data Privacy Officer, CIPP/E etc.).

Haftung der Datenschutzberaterin

Die Datenschutzberaterin kann eine Angestellte des Verantwortlichen sein und muss wie oben beschrieben entsprechend unabhängig in der Organisation agieren können. Es kann aber auch eine externe Person für diese Aufgabe berufen werden. Auch externe Personen müssen die oben beschriebenen Aufgaben erfüllen, und auch ihr müssen die entsprechenden Mittel und Kompetenzen zugestanden werden.

HINWEIS

Aus der Beratungstätigkeit lässt sich feststellen, dass (kleinere) KMU eine (interne) Person in der Datenschutzerklärung als «zuständige Person», «Datenschutzverantwortliche» oder «Datenschutzberater» nennen. Dabei ist oft unklar, welche Rolle diese Person tatsächlich innehat resp. ob dieser Person tatsächlich die Rolle der Datenschutzberaterin zukommt. Oft verfügen diese Personen weder über die erforderlichen Fachkenntnisse, noch sind sie organisatorisch richtig eingegliedert, um unabhängig die Rolle der Datenschutzberaterin wahrnehmen zu können. Es empfiehlt sich für kleinere KMU, die internen Rollenverteilungen zu überprüfen und Personen ohne entsprechende Fachkenntnisse von diesen Positionen zu befreien.

Das DSG kennt ein verschärftes Haftungsregime, es gibt einen Sanktionenkatalog mit empfindlichen Bussen (wobei es zu betonen gilt, dass nur bei Vorsatz und auf Antrag geahndet wird – siehe *WEKA Datenschutz Newsletter Ausgabe März 2023, das Sanktionenregime des revidierten Datenschutzgesetzes).* Bezüglich der Sanktionen ist für die Schweiz relativ neu, dass nicht das fehlbare Unternehmen, sondern eine natürliche Person haftet. Das heisst im Grundsatz, dass die Geschäftsleitung (CEO) oder der Verwaltungsrat (VRP) zur Verantwortung gezogen wird. Wurde jedoch eine (interne oder externe) Datenschutzberaterin bestimmt, kann diese Person unter Umständen direkt haftbar sein. Dies wird wohl dann der Fall sein, wenn die Datenschutzberaterin die Verantwortliche wissentlich und willentlich in einer Verletzung von Datenschutzvorschriften unterstützt oder daran mitgewirkt hat. Dieses Szenario wird wohl eher die Ausnahme als die Regel bilden. Wie oben beschrieben, muss der Datenschutzberaterin die Kompetenz eingeräumt werden, bei wichtigen Fällen das oberste Organ zu benachrichtigen. Ein solcher Fall kann beispielsweisedie drohende oder bereits erfolgte Datenschutzverletzung durch das Unternehmen sein. Wenn jedoch Entscheidungen gefällt werden, die zu Datenschutzverletzungen führen und die ohne Wissen oder entgegen den Empfehlungen der Datenschutzberaterin zustande kommen, dann kann die Datenschutzberaterin hierfür nicht ohne Weiteres haftbar gemacht werden.

Sollte der Verantwortliche gebüsst werden, sind für die interne Datenschutzberaterin allenfalls noch arbeitsrechtliche und für die externe Datenschutzberaterin auftragsrechtliche Aspekte zu beachten. Zu denken ist z. B. an Rückgriffe aufgrund arbeitsvertraglicher oder auftragsrechtlicher Sorgfaltspflichtverletzungen, da in diesen Fällen die Haftung bereits bei Fahrlässigkeit greifen kann. Es lohnt sich auf jeden Fall, die entsprechenden Besonderheiten im Auftragsverhältnis oder Arbeitsvertrag explizit festzuhalten. Empfehlenswert sind sicherlich auch Versicherungslösungen, um die Risiken für die Datenschutzberaterin abzufedern (in der Regel laufen diese unter der Organhaftpflichtversicherung).

Fazit

Die Datenschutzberaterin haftet wohl nur im Ausnahmefall für Datenschutzverletzungen der Verantwortlichen. Sie ist aber aufgrund ihrer Aufgabenfelder und Kompetenzen angehalten, entsprechenden Verletzungen entgegenzuwirken und bei wichtigen Fällen das oberste Organ zu informieren. Die letzte Entscheidungskompetenz liegt jedoch nicht bei der Datenschutzberaterin. Es empfiehlt sich, die besondere Stellung der Datenschutzberaterin im Arbeitsvertrag oder Auftragsverhältnis inkl. Haftungsfragen und Versicherungslösungen festzuhalten.

AUTORIN

Eleonor Gyr, Dr. iur., Rechtsanwältin, CIPP/-E, ist spezialisiert auf IT-, Gesellschafts- und Finanzmarktrecht und Partnerin der Wirtschaftskanzlei Gyr | Gössi | Olano | Staehelin in Basel.

Unterzeichnung der Datenschutzerklärung durch Mitarbeitende – ist das wirklich notwendig?

Rund um die Datenschutzerklärung für Mitarbeitende bestehen viele Unsicherheiten und datenschutzrechtliche Mythen, welche weit verbreitet sind und sich hartnäckig halten. Eine dieser Unsicherheiten besteht bei der Frage, ob es aus rechtlicher Sicht ausreicht, wenn die Datenschutzerklärung den Mitarbeitenden zur Einsicht zur Verfügung gestellt wird, oder ob diese unterzeichnet werden muss. Dieser Frage gehen wir in diesem Beitrag nach.

Von Anna Neukom Chaney und Marco S. Meier

Hintergrund

Seit dem 1. September 2023 gilt das totalrevidierte Datenschutzgesetz (DSG) in der Schweiz. Mit dem DSG wurden verschiedene neue Pflichten für Unternehmen eingeführt, welche Personendaten bearbeiten. Obwohl gerade Datenbearbeitungen in der eigenen Personalabteilung mit erhöhten Risiken einhergehen, werden diese zuweilen etwas vernachlässigt. Denn: Nebst den «normalen» Personendaten (wie z. B. Namen der Mitarbeitenden, Personalnummer, Finanzdaten, etc.) werden im HR regelmässig auch besonders schützenswerte Daten (z. B. Strafregisterauszüge, Arztzeugnisse, etc.) bearbeitet. In Bezug auf die Bearbeitung von Personendaten sieht das DSG vor, dass die betroffenen Personen über die Bearbeitung der Personendaten informiert werden müssen. Das gilt auch für die Bearbeitungen im Rahmen des Anstellungsverhältnisses.

Die Informationspflicht ist eine derjenigen Pflichten des DSG, welche bei vorsätzlicher Verletzung direkt sanktioniert werden kann. Wird den Mitarbei-

tenden vorsätzlich eine falsche oder unvollständige Auskunft erteilt, kann die verantwortliche Person (und nicht das Unternehmen) mit einer Busse von bis zu CHF 250 000.– gebüsst werden.

Mindestinhalt der Information

Das DSG sieht für die Information, die den Mitarbeitenden zur Verfügung gestellt werden muss, folgenden Mindestinhalt vor:

- Die Information muss klar offenlegen, wer für die Bearbeitung verantwortlich ist und wie die Verantwortliche kontaktiert werden kann (d. h. den Namen und die Kontaktangaben des Arbeitgebers).
- Die verschiedenen Bearbeitungszwecke der Datenbearbeitungen müssen transparent gemacht werden (z. B. Führung des Personaldossiers, Aus- und Weiterbildungsplanung, Arbeitsplanung, Verrechnung, Abschluss von Versicherungen etc.).
- Sofern Daten an Dritte weitergegeben werden, müssen diese offengelegt werden (z. B. cloudbasiertes Personaladministrationstool, Payroll-Provider, Versicherungen etc.).
- Werden die Daten ins Ausland übertragen, müssen zusätzlich der Staat, an den die Daten übertragen werden, sowie die datenschutzrechtliche Garantie zur Sicherstellung eines angemessenen Datenschutzniveaus (z. B. die EU-Standardvertragsklauseln) offenbart werden.

In der Praxis werden regelmässig noch detailliertere Informationen zur Verfügung gestellt, so z. B. Kategorien der bearbeiteten Personendaten (wie Kontaktangaben, Lohndaten, Finanzdaten etc.).

Modalitäten der Information

Das DSG selbst macht nur vage Angaben zu den Modalitäten der Informationspflicht. Es hält namentlich einzig fest, dass die betroffenen Personen angemessen über die Beschaffung von Personendaten informiert werden müssen. Die Verordnung zum DSG führt zu den Modalitäten der Informationspflicht aus, dass die Information präzise, transparent, verständlich und leicht zugänglich sein muss. Mit anderen Worten muss die Information für die Mitarbeitenden in einfacher Sprache und adressatengerecht abgefasst werden.

In der Praxis wird dies über eine spezifische Datenschutzerklärung für die Mitarbeitenden sichergestellt. Gelegentlich stösst man in Bezug auf die Datenschutzerklärung für Mitarbeitende auf die Meinung, dass eine solche nicht notwendig sei. Argumentiert wird dies über eine im DSG enthaltene Ausnahme von der Informationspflicht. Die Informationspflicht entfällt beispielsweise dann, wenn die Bearbeitung gesetzlich vorgesehen ist. Im Rahmen des Arbeitsverhältnisses gibt es tatsächlich Bearbeitungen, welche gesetzlich vorgesehen sind (z. B. die Abrechnung von Sozialversicherungsbeiträgen, der Abschluss von bestimmten Versicherungen etc.). Folglich müsste über solche Bearbeitungen nicht informiert werden. Dies greift u. E. aber zu kurz. Denn neben den gesetzlich vorgesehenen bestehen regelmässig andere Bearbeitungen, welche durch die Arbeitgeberin durchgeführt werden, die nicht zwingend auf einer gesetzlichen Grundlage fussen. Insofern müssen die Mitarbeitenden (mindestens) über die nicht vom Gesetz vorgesehenen Bearbeitungen informiert werden. Empfehlenswert ist es, diesbezüglich aber eine vollständige Information zu erstellen, die ggf. auch die gesetzlich vorgesehenen Bearbeitungen transparent macht. Das schafft gegenüber den Mitarbeitenden ganz nach dem Motto «wenn schon, denn schon» nicht nur Transparenz, sondern hilft ihnen umfassend zu verstehen, wie das HR Personendaten bearbeitet.

Unterzeichnung? Nicht notwendig

Das DSG und dessen Verordnung schreiben nicht konkret vor, wie die Datenschutzerklärung den Mitarbeitenden zur Verfügung gestellt werden muss. Zentral ist aber, dass die Datenschutzerklärung leicht zugänglich ist. Sie kann folglich beispielsweise im Intranet aufgeschaltet, per E-Mail versandt, im Welcome-Package enthalten sein oder im Pausenraum angeschlagen werden.

Anders als z. B. beim Arbeitsvertrag oder dem Personalreglement handelt es sich bei der Datenschutzerklärung um eine einseitige Information und nicht um einen Vertrag oder einen Vertragsbestandteil. Somit kann festgehalten werden, dass die Datenschutzerklärung keiner Unterschrift bedarf. Der datenschutzrechtliche Mythos kann damit entkräftet werden.

HINWEIS

Das Wichtigste in Kürze:

- Das DSG sieht eine Informationspflicht mit Mindestinhalt vor.
- Den Mitarbeitenden muss eine Datenschutzerklärung, welche die Bearbeitungen während des Arbeitsverhältnisses abbildet, zur Verfügung gestellt werden.
- Die Datenschutzerklärung ist eine einseitige Information und kein Vertrag.
- Die Datenschutzerklärung muss den Mitarbeitenden «nur» zur Kenntnisnahme zur Verfügung gestellt werden. Eine Unterzeichnung durch die Mitarbeitenden ist gesetzlich nicht vorgesehen und darum nicht notwendig.

AUTOREN

Anna Neukom Chaney, RAin, lic. iur., Fachanwältin SAV Arbeitsrecht, ist Partnerin bei THOUVENIN Rechtsanwälte KLG. Sie berät und vertritt Arbeitgeber sowie Mitarbeitende in allen Belangen des Arbeitsrechts und verfügt über umfangreiche Prozesserfahrung.

Marco S. Meier, RA, MLaw, CIPP/E, ist Counsel bei THOUVENIN Rechtsanwälte KLG. Seine Tätigkeitsschwerpunkte liegen im Datenschutz- und IT-Recht sowie in technologiebezogenen Compliance-Fragen.

Das Datenschutzgesetz gilt nicht für den B2B-Bereich – trifft das zu?

Von irgendwoher stammt die Anmutung, dass Datenschutz nur etwas mit Menschen zu tun haben will, nicht aber mit Unternehmen. Ganz falsch ist dies nicht. Datenschutzrecht ist Persönlichkeitsschutz. In der Tat ist dieses vornehmlich auf natürliche Personen zugeschnitten. Was dabei aber vergessen geht: Die Rechtsprechung des Schweizer Bundesgerichts hat den Persönlichkeitsschutz in der Vergangenheit auch juristischen Personen zugesprochen. Auch Letztere haben eine «Persönlichkeit». Was ebenfalls gerne vergessen geht: Unternehmen (Businesses abgekürzt mit «B») bestehen auch nur aus Menschen. Wenn zwei Unternehmen miteinander kommunizieren, tun sie dies in der Regel durch zwei Menschen, nicht zwei Unternehmen. Und schon werden zwischen diesen Unternehmen natürliche Personendaten ausgetauscht. Der nachfolgende Beitrag geht dem Mythos nach, das DSG gelte nicht für den B2B-Bereich. Es zeigt auf, wo diese Annahme scheitert und wo sie möglicherweise doch zutrifft.

Von Dirk Spacek

Daten natürlicher und juristischer Personen

Die Normen der europäischen DSGVO bezwecken den Schutz natürlicher Personen bei der Bearbeitung personenbezogener Daten. Sie gilt nicht für die Bearbeitung personenbezogener Daten juristischer Personen, einschliesslich deren Namen, Rechtsform oder Kontaktdaten.[1] Auch das revidierte Datenschutzgesetz vom September 2023 ist nur noch auf den Schutz personenbezogener Daten natürlicher Personen ausgerichtet.[2] Auf den Schutz von Daten juristischer Personen wurde im Rahmen der Revision verzichtet, weil dieser im Umfeld der EU und des Europarats eine Ausnahme darstellt. Zudem war der Schutz dieser Daten unter dem alten DSG von geringer praktischer Bedeutung. Der Schutz juristischer Personendaten wird vielmehr durch andere Bestimmungen gewährleistet wie z. B. Geschäftsgeheimnisse und insbesondere auch durch den allgemeinen Persönlichkeitsschutz gemäss Art. 28 ZGB. Juristische Personen geniessen damit zumindest teilweise auch den Persönlichkeitsschutz von Art. 13 BV.[3] Allerdings entfällt das Auskunftsrecht für juristische Personen, dieses ist nur natürlichen Personen zugänglich.

Der Business-to-Business-Kontext («B2B»)

Sind nun zwei Unternehmen in geschäftlichem Kontakt, liegt die (falsche) Vermutung nahe, es lägen zwei juristische Personen vor, das Datenschutzgesetz sei mithin nicht anwendbar. Diese Sichtweise greift natürlich viel zu kurz. Neben dem Schutz der Daten einer juristischen Person sind zahlreiche Konstellationen denkbar, in welchen Daten natürlicher Personen zwischen Unternehmen erhoben, ausgetauscht, bearbeitet oder bekannt gegeben werden. Zu denken ist an Mitarbeiterkontaktdaten als auch an Kundendaten. Das Datenschutzgesetz findet immer dann Anwendung, wenn Personendaten bearbeitet werden. Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.[4] Eine Bearbeitung liegt bei jedem Umgang mit Personendaten vor, dazu gehören beispielsweise das Beschaffen, Aufbewahren, Bekanntgeben oder Löschen von Daten.[5] Insofern ist bereits eine E-Mail-Adresse wie eine Unternehmens-E-Mail, die den Vor- und Nachname der betroffenen Person enthält, vom Datenschutzgesetz erfasst. Nicht erfasst wäre eine anonyme Unternehmensadresse wie beispielsweise z. B.[6] info@... .[7] Somit ist auch im B2B-Kontext das Datenschutzgesetz zu beachten, wenn personenbezogene Daten bearbeitet werden. Die Qualifikation der bearbeiteten Daten ist entscheidend, nicht der Kontext des Austausches (B2B).

Wenn das Business Personendaten von einem anderen Business übermittelt erhält und bearbeitet

Erhält ein Unternehmen Personendaten von einem anderen Unternehmen für eigene Zwecke übermittelt,

1 Erwägungsgrund 14 DSGVO; EDPB, Leitlinien 2/2018 zum räumlichen Anwendungsbereich der DSGVO (Art. 3), Version 2.0, 12. November 2019, Ziff. 2.a.

2 Art. 5 lit. a DSG.

3 BBl 2017 6972.

4 Art. 5 lit. a DSG.

5 Art. 5 lit. d DSG.

6 www.gdprregister.eu/gdpr/gdpr-b2b-marketing/

7 www.gdprregister.eu/gdpr/gdpr-b2b-marketing/

so muss dieses die betroffene Person über den Zweck der Bearbeitung, die Identität des Verantwortlichen und die Kategorien der bearbeiteten Personendaten grundsätzlich informieren. Die Informationspflicht gilt grundsätzlich zwischen jedem Verantwortlichen und Betroffenen, und zwar auch dann, wenn die Daten nicht bei der betroffenen Person selbst beschafft wurden.[8] Anders zu beurteilen wäre der Fall, wenn ein Unternehmen Daten nur für Bearbeitungszwecke übermittelt erhält. Diesfalls ist das empfangende Unternehmen ein Datenbearbeiter, der Daten nur für fremde Zwecke (im Auftrag) bearbeitet. Er hat keine direkten Informationspflichten gegenüber den betroffenen Personen.

Wenn das Business Geschäftskontakte eines anderen Business speichert und Marketing betreibt

Der Schutz personenbezogener Daten erfolgt unabhängig davon, ob die Daten aufgrund einer Geschäftsbeziehung oder auf anderem Wege erhoben werden. Die Unterscheidung spielt höchstens bei Rechtfertigungsgründen einer Datenbearbeitung kontextuell eine Rolle.[9] Das bedeutet, dass bereits bei der Verwaltung von Kontaktdaten von Ansprechpartnern und Geschäftskunden Datenschutzbestimmungen grundsätzlich zu beachten sind, denn es sind wie gesagt Daten von Menschen, die abgespeichert werden (natürliche Personendaten von Mitarbeitern). Auch im B2B-Marketing sind diese Bestimmungen genauso zu beachten. Die im DSG festgelegten Bearbeitungsgrundsätze sind dabei zu beachten (Verhältnismässigkeit, Zweckbindung, Erkennbarkeit, Datensicherheit etc.).[10] Geschäftskontakte sollten grundsätzlich darüber informiert werden, dass ihre personenbezogenen Daten erhoben werden und mit wem sie geteilt werden.[11] Zusätzlich legt das SPAM-Verbot in Art. 3 Abs. 1 lit. o. UWG fest, dass im Falle automatisierter Massenwerbung an solche Empfänger sowohl ein vormaliges Opt-in (Einwilligung) als auch ein jederzeitiges Opt-out (über einen Unsubscribe-Button) möglich sein muss.

Wenn das Business Daten zu einem anderen Business für Bearbeitungszwecke auslagert (Outsourcing)

Eine weitere häufige Konstellation, in der die Datenschutzbestimmungen im B2B-Verhältnis zu beachten sind, ist das Auftragsbearbeitungsverhältnis. Hier bearbeitet ein Unternehmen als Auftragnehmer Personendaten für ein anderes Unternehmen als Auftraggeber. Der Auftraggeber bleibt jedoch der Verantwortliche im Sinne des Datenschutzgesetzes. Die beteiligten Unternehmen müssen hierzu eine Vereinbarung abschliessen. So muss der Auftraggeber sicherstellen, dass der Auftragnehmer die Daten nur im Auftrag und in dem Umfang bearbeitet wie vom Auftraggeber vorgegeben.[12] Der Auftraggeber hat in der Regel umfassende Auditrechte. Bestimmungen zur allfälligen Bearbeitung im Ausland sind zu vereinbaren.

8 Art. 19 DSG siehe auch Ausnahmen in Art. 20.

9 Art. 31 DSG.

10 Art. 6 DSG.

11 https://usercentrics.com/knowledge-hub/how-does-gdpr-affect-b2b-sales/#:~:text=Does%20the%20GDPR%20protect%20B2B,the%20data%20is%20used%20for

12 Art. 9 DSG.

Weiter sind die Anforderungen an die Datensicherheit insbesondere die zu treffenden technischen und organisatorischen Massnahmen, vertraglich festzuhalten.[13] Das Datenschutzgesetz schreibt weiter vor, dass der Auftragnehmer den Auftraggeber unverzüglich über eine Verletzung der Datensicherheit zu informieren hat.[14] Auch Auskunftsbegehren von betroffenen Personen sind vom Auftragnehmer an den Verantwortlichen weiterzuleiten. Die Auskunftspflicht bleibt beim Verantwortlichen.[15] Die Verletzungen der Informations-, Auskunfts- oder auch Sorgfaltspflichten kann mit Bussen bis zu CHF 250 000.– bestraft werden.[16] Man sieht: Auch wenn wir uns im B2B-Kontext bewegen, gilt das DSG, und die Pflicht zur Regelung von Auftragsdatenbearbeitungen besteht.

ZUSAMMENFASSUNG

- ✓ Für die Anwendbarkeit des DSG ist die Qualifikation von Daten entscheidend. Liegen personenbezogene Daten natürlicher Personen (d. h. identifiziert oder nach den Umständen identifizierbar) vor? Dann lässt sich der Anwendungsbereich des DSG nicht wegdiskutieren.
- ✓ Der Kontext von Sachverhalten (B2B oder B2C) ist nicht entscheidend für Sachfragen des Datenschutzes. Entscheidend ist, welche Art/Kategorie von Daten gegenständlich sind bzw. in diesen Kontexten ausgetauscht und bearbeitet werden.
- ✓ Im B2B-Kontext können Personendaten genauso bearbeitet werden wie im B2C-Kontext. Auch Unternehmen speichern, bearbeiten und tauschen Personendaten aus.
- ✓ Die datenschutzrechtlichen Pflichten des DSG sind deshalb auch zwischen Unternehmen zu beachten. Transparenz/Information, Zweckbindung, Datensicherheit, Auftragsdatenbear-beitungsverträge, Auslandsdatentransferverträge (wo nötig), das ganze Spektrum ist zu beachten.
- ✓ Es besteht im B2B-Kontext oft eine tiefere Quantität an personenbezogenen Daten. Nicht immer, nicht zwingend, aber oft werden nicht-personenbezogene (Geschäfts-) Daten ausgetauscht. In solchen Konstellationen besteht eine tiefere Risikoexponiertheit vor dem DSG. Allerdings könnten solche Daten ebenfalls sensitiv sein, z.B. können sie wertvolle Geschäftsgeheimnisse darstellen und sollten ebenfalls mit angemessenen Schutzmechanismen vor unbefugtem Gebrauch geschützt werden (z.B. mit Non-Disclosure-Agreements [«NDAs»] sowie mit einem hausinternen Berechtigungsregime, das solche Information vor exzessiver Verwendung und Preisgabe schützt).

Wenn das Business Daten an andere Unternehmen (im Ausland) weitergibt

Gibt ein Unternehmen Personendaten an ein anderes Unternehmen im Ausland bekannt, liegt ein Auslandsdatentransfer vor. In solchen Konstellationen sind die Bestimmungen von Art. 16 DSG zu beachten. Daten dürfen nur ins Ausland bekannt gegeben werden, wenn im Empfängerstaat ein angemessener Schutz besteht. Liegt kein solcher Schutz im Ausland und auch kein offizieller Angemessenheitsbeschluss vor, ist ein Transfer an das ausländische Unternehmen nur möglich, wenn die betroffene Person darüber informiert wurde und im Voraus eingewilligt hat oder ein sogenannter Datentransfervertrag unter den EU-Standardvertragsklauseln abgeschlossen wurde. Die Europäische Kommission hat am 15. Januar 2024 festgestellt, dass die Schweiz über ein angemessenes Datenschutzniveau verfügt.[17] In den USA besteht aus Sicht der Schweiz kein angemessener Schutz von Personendaten.[18] Insbesondere von Software sind viele der Hersteller in den USA ansässig.[19] Die EU hat inzwischen einen Angemessenheitsbeschluss für das EU-USA Data Privacy Framework gefasst.[20] Gespräche zur Erstellung eines vergleichbaren Swiss-US Data Privacy Framework sind in der Schweiz pendent.[21] Auch wenn wir uns also in einem B2B-Kontext bewegen, ist das DSG anwendbar, sobald Personendaten zwischen Unternehmen landesübergreifend ausgetauscht werden.

Sind B2B und B2C demzufolge genau das Gleiche aus Sicht des DSG?

Nein, nicht ganz. Zweifellos werden im B2B-Kontext quantitativ weniger personenbezogene Daten ausgetauscht – zumindest in den meisten Konstellationen – als in einem B2C-Kontext. Ein grosser Teil der ausgetauschten Daten sind in der Regel nicht personenbezogene Business-Daten (z. B. Pläne, Kalkulationen, Geschäftspläne oder Verträge für ein geplantes Projekt). Dies dürfte in einem B2C-Kontext anders sein, denn hier steht der Austausch von personenbezogenen Endkundendaten im Vordergrund. Insofern kann man sagen, dass die datenschutzrechtliche Exponiertheit und die Risiken im B2B-Kontext möglicherweise tiefer liegen. Doch es wäre ein Trugschluss anzunehmen, das Datenschutzgesetz gälte im B2B-Kontext grundsätzlich nicht.

13 Art. 8 DSG; Art. 1 ff. DSV.
14 Art. 24 Abs. 3 DSG.
15 Art. 25 Abs. 4 DSG.
16 Art. 60 und 61 DSG.
17 www.edoeb.admin.ch/dam/edoeb/de/Dokumente/datenschutz/20240115%20EC%20Adequacy%20decision%20DE.pdf.download.pdf/20240115%20EC%20Adequacy%20decision%20DE.pdf
18 Matthias Schönbächler ZBJV 159/2023, 171 ff., 183; BBL 2017 6998; Anne-Sophie Marand/Selma Duc, International data transfers and the EU's adequacy decisions, in: Jusletter 3. Mai 2021.
19 Matthias Schönbächler ZBJV 159/2023, 171 ff., 18.
20 https://ec.europa.eu/commission/presscorner/detail/de/ip_23_3721
21 www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/2023/20230410_eu_us_dpf.html

AUTOR

Dirk Spacek, Dr. iur., LL.M., ist Partner in der internationalen Anwaltskanzlei CMS (Schweiz). Er ist Spezialist für Medien-, Technologie-(IT-) und Immaterialgüterrecht. Er berät Unternehmen vorwiegend in technologieaffinen Rechtsfragen.

«Betroffene Personen haben nur das Recht auf Auskunft, mehr nicht» – stimmt das denn wirklich?

Durch das am 1. September 2023 in Kraft getretene neue Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) sollen unter anderem auch die Rechte betroffener Personen gestärkt werden. Das revidierte Datenschutzgesetz soll Individuen mehr Kontrolle über ihre Daten geben und sicherstellen, dass Unternehmen transparent und verantwortungsvoll mit erlangten Daten umgehen. Das vierte Kapitel des DSG widmet sich den Rechten betroffener Personen. Diesen räumt das Datenschutzgesetz das Recht auf Auskunft (Art. 25 DSG) und das Recht auf Datenherausgabe und -übertragung (Art. 28 DSG) ein. Das fünfte Kapitel des DSG gewährt den betroffenen Personen weitere Rechtsansprüche (Art. 32 DSG). Betroffene Personen haben damit mehr Möglichkeiten, auf die sie zurückgreifen können, als bloss das Auskunftsrecht.

von Alesch Staehelin

Was umfasst das Auskunftsrecht?

Das Auskunftsrecht gibt den betroffenen Personen das Recht, Auskunft darüber zu verlangen, ob die Verantwortliche Personendaten über sie bearbeitet. Folgende Mindestinformationen müssen erteilt werden:

- Identität und Kontaktdaten der Verantwortlichen
- die bearbeiteten Personendaten als solche
- Bearbeitungszweck
- Aufbewahrungsdauer der Personendaten (soweit unmöglich, die Kriterien zum Festlegen der Dauer)
- verfügbare Angaben über die Herkunft der Personendaten (soweit diese nicht bei der betroffenen Person beschafft wurden)
- Vorliegen einer automatisierten Einzelentscheidung und die Logik, auf der diese Entscheidung beruht
- Empfänger oder Kategorien von Empfängern, denen Personendaten bekannt gegeben werden

Die Auskunftserteilung erfolgt grundsätzlich kostenlos. Nur bei einem unverhältnismässig hohen Aufwand darf die auskunftsersuchende Person an den Kosten beteiligt werden. Die Verantwortliche hat 30 Tage Zeit, um auf eine Auskunftsanfrage zu antworten.

Was bringt das Recht auf Datenherausgabe?

Alle betroffenen Personen haben das Recht, die Herausgabe von Personendaten, die der Verantwortlichen bekannt gegeben wurden, in einem gängigen elektronischen Format herauszuverlangen. Durch die Datenherausgabe wird der Verantwortlichen die Datenbearbeitung aber nicht untersagt. Soweit ein Rechtfertigungsgrund vorliegt, kann die Verantwortliche die Daten weiterhin bearbeiten. Der Anspruch auf Datenherausgabe besteht, soweit zwei Voraussetzungen kumulativ erfüllt sind: Erstens muss es sich um eine automatisierte Bearbeitung handeln. Zweitens muss diese automatisierte Bearbeitung aufgrund einer Einwilligung erfolgen oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen der Verantwortlichen und der betroffenen Person stehen. Wird der Anspruch gel-

WICHTIGER HINWEIS

Kein eigenständiges Recht auf Löschung bzw. «Vergessenwerden»: Was muss ich wissen?

Das Datenschutzgesetz sieht kein explizites Recht auf Löschung der Daten vor. Deshalb verweist es im Rahmen des Berichtigungsrechts auf die zivilrechtlichen Klagen zum Schutz der Persönlichkeit gemäss Art. 28 Zivilgesetzbuch (ZGB), Art. 28a ZGB und Art. 28 g–l ZGB. Die von einer Personendatenbearbeitung betroffene Person hat damit die Möglichkeit, gegen die «an der Verletzung mitwirkende Person» – also Verantwortliche sowie Auftragsbearbeiter und andere Hilfspersonen – zivilgerichtlich und klageweise vorzugehen. Es bestehen folgende zivilrechtliche Ansprüche:

- negatorische Ansprüche
  - Unterlassungsklage
  - Beseitigungsklage
  - Feststellungsklage
- reparatorische Ansprüche
  - Schadensersatz
  - Genugtuung
- Gewinnherausgabe
- Gegendarstellungsrecht

tend gemacht, hat die Verantwortliche 30 Tage Zeit, die Daten herauszugeben. Ähnlich wie beim Auskunftsrecht müssen die Daten kostenlos herausgegeben werden (es sei denn, der Bundesrat hat ausdrücklich eine Ausnahme von dieser Regelung vorgesehen). Das gängige elektronische Format wird im Datenschutzgesetz nicht weiter spezifiziert.

Worum geht es beim Recht auf Datenübertragung?

Das Recht gewährt der betroffenen Person den Anspruch, gegenüber der Verantwortlichen eine Übermittlung der Daten an eine andere Verantwortliche zu erwirken. Der Anspruch besteht, soweit ein Anspruch auf Herausgabe der Daten anzunehmen ist und die Übermittlung keinen unverhältnismässigen Aufwand erfordert. Das Vorliegen eines unverhältnismässigen Aufwands dürfte dabei nur in Ausnahmefällen anzunehmen sein. Im Zusammenhang mit dem Geltendmachen des Rechts auf Datenübertragung ist in der Praxis zu berücksichtigen, dass die (andere) Verantwortliche, an die die Daten übertragen werden sollen, rechtlich nicht dazu verpflichtet ist, den Empfang übertragener Daten anzubieten. Bietet die Empfängerin dies nicht an, läuft ein Geltendmachen des Anspruchs auf Datenübertragung ins Leere.

Das Recht auf Berichtigung und der sogenannte Bestreitungsvermerk

Das Recht auf Berichtigung räumt der betroffenen Person das Recht ein, die Berichtigung falscher Personendaten zu verlangen. Dieser Berichtigungsanspruch besteht nicht, soweit eine gesetzliche Vorschrift die Änderung der Personendaten verbietet oder die Personendaten zu Archivzwecken im öffentlichen Interesse bearbeitet werden. Das Berichtigungsrecht ergänzt den Bearbeitungsgrundsatz sowie die damit einhergehenden Pflichten der Datenbearbeiter, insbesondere die Pflicht, die Richtigkeit und Aktualität der Personendaten zu gewährleisten. Zum Ermitteln der Unrichtigkeit der Daten muss der Bearbeitungszweck berücksichtigt werden und eine umfassende Abwägung im Einzelfall stattfinden. Im Übrigen ist zu beachten, dass auch die Unvollständigkeit der Daten zur Unrichtigkeit führen kann. Sollte, weder die Unrichtigkeit noch die Richtigkeit der bearbeiteten Daten beweisbar sein, kann die betroffene Person das Anbringen eines sogenannten Bestreitungsvermerks verlangen. Die praktische Bedeutung dieses Vermerks dürfte gering sein.

Wobei hilft das Widerspruchsrecht?

Betroffene Personen können einer Bearbeitung von Personendaten widersprechen. Erfolgt dennoch eine Bearbeitung der Personendaten, ist gemäss dem Gesetzgeber bereits eine hinreichende Intensität gegeben, sodass von einer Persönlichkeitsverletzung auszugehen ist. Erforderlich ist jedoch eine

«ausdrückliche Willenserklärung» der betroffenen Person. Überdies kann der Bearbeiterin das Bearbeiten von Daten ohne weitere Voraussetzungen und ohne Interessensnachweis verboten werden (sog. Opt-out-Prinzip). Eine Persönlichkeitsverletzung kann jedoch ausnahmsweise gerechtfertigt sein. In solchen Fällen steht der Widerspruch der Bearbeitung nicht entgegen.

AUTOR

Alesch Staehelin ist Rechtsanwalt in Zürich und als Partner der Kanzlei Uto Legal (utolegal.ch) in den Bereichen «Data, IT/IP & Media» tätig: Er berät in Fragen des Datenschutzes, der IT-Sicherheit, der digitalen Transformation, der neuen Technologien (KI, IoT, VR, AR usw.), der sozialen Medien, des E-Commerce, von ESG, des Urheber-, Unterhaltungs- und Medienrechts, des Marken-, Design- und Patentrechts (inkl. Know-how-Schutz) sowie des Wettbewerbsrechts, er entwirft, prüft und verhandelt Verträge aller Art (insbesondere in komplexen, zeitkritischen und grenzüberschreitenden Tech-Deals), er vermittelt in strittigen Projekten, und er führt Gerichts- und Schiedsverfahren. Zuvor leitete Alesch Staehelin seine eigene Kanzlei, und er war über ein Jahrzehnt Partner in einer anderen schweizerischen Anwaltskanzlei sowie Senior Corporate Counsel in diversen Managementfunktionen bei IBM.

Vorlage für Abonnenten dieses Newsletters kostenlos

Diese Mustervorlage stammt aus dem Online-Modul «Datenschutz kompakt». Als Abonnent haben Sie Zugriff auf diese sowie auf zahlreiche weitere Vertragsvorlagen und rechtliche Musterbriefe. Falls Sie Abonnent dieses Print-Newsletters sind und die Vorlage gerne kostenlos zugesandt haben möchten, schreiben Sie uns eine kurze E-Mail (joel.weishaupt@weka.ch), und wir senden Ihnen die Vorlage umgehend zu.

Datenschutzerklärung für die Website gemäss DSG

Datenschutzerklärung für die Website

1. Wichtiger Hinweis

Diese Datenschutzerklärung ist auf eine „einfache" Datenbearbeitung kleinerer und mittlerer Schweizer Unternehmungen als Muster im Anwendungsbereich des neuen Schweizer Bundesgesetzes über den Datenschutz[1] (DSG) zugeschnitten. Bei der praktischen Anwendung ist jeweils auf den konkreten Anwendungsfall im Unternehmen abzustellen und die Datenerhebung samt dem gesamten Datenbearbeitungszyklus (wie Datenbeschaffung, Datenbearbeitungszweck, Datenweitergabe und Datenübermittlung) in verständlicher und klarer Weise zu beschreiben.

Ferner wird darauf hingewiesen, dass diese Datenschutzerklärung die Mindestanforderungen der Informationspflicht gemäss Art. 19 DSG enthält. Je nach Art der bearbeiteten Daten (sensible oder nicht sensible Daten), des Umfangs (Menge der Datensätze), der Umstände und des Zwecks der fraglichen Datenbearbeitung, muss der Verantwortliche umfassender informieren. Zu den Informationen, welche bei einer umfassenden Information zusätzlich angegeben werden müssen, gehören beispielsweise Angaben zur Dauer der Datenbearbeitung, der Datenquelle, der Rechtsgrundlage, zu einem spezifischen Datenempfänger oder zu den Betroffenenrechten, wie dies das EU-Recht zwingend vorsieht. Solche Zusatzangaben sind vor allem in Fällen notwendig, bei denen eine hohe Gefahr einer Persönlichkeitsverletzung besteht, um der betroffenen Person dadurch eine bessere Abschätzung der damit verbundenen Risiken zu ermöglichen und die Wahrnehmung der Betroffenenrechte sicherzustellen. Zusatzangaben, welche die betroffene Person nicht interessieren, müssen hingegen nicht gemacht werden (vgl. dazu auch die Ausführungen zur Informationspflicht nach schweizerischem Datenschutzrecht). Auf was vorliegend nicht darauf eingegangen wird, sind die Ausnahmen der Informationspflicht und Einschränkungen nach Art. 20 DSG. Diese müssen jeweils im konkreten Fall separat geprüft werden.

Diese Datenschutzerklärung stellt keine rechtliche Beratung dar und ist eine unverbindliche, nicht abschliessende Mustervorlage für eine Information über die Datenbearbeitung nach Art. 19 DSG. Für die Richtigkeit, Vollständigkeit und Aktualität des bereitgestellten Musters sowie auch für weiterführende Links kann aufgrund der derzeitigen Entwicklungen im Datenschutzrecht mit unterschiedlichen Anforderungen, Begriffsdefinitionen und Anwendungen in der Schweiz sowie eines möglichen internationalen Bezugs der Bearbeitungstätigkeit keine Gewähr übernommen werden. Um das Risiko von Bussgeldern bei einer Verletzung zu vermeiden bzw. zu reduzieren, ist eine Zusammenarbeit mit einer Rechtsanwältin/einem Rechtsanwalt Ihres Vertrauens für die massgeschneiderte Ausarbeitung und Prüfung der Datenschutzerklärung und der Datenbearbeitungen geboten.

2. Informationspflicht nach Art. 19 DSG

Die gesetzliche Formulierung von Art. 19 DSG sieht vor, dass:

1. der Verantwortliche die betroffene Person *angemessen* über die Beschaffung von Personendaten zu informieren hat; dies gilt auch, wenn die Personendaten nicht bei der betroffenen Person beschafft werden.
2. Er hat der betroffenen Person bei der Beschaffung diejenigen Informationen mitzuteilen, die erforderlich sind, damit sie *ihre Rechte* nach dem neuen Datenschutzgesetz geltend machen

[1] Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG), rechtskräftig per 1. September 2023.

WEKA Business Media AG | www.weka.ch | Autorin: Regina Arquint 1/22

IMPRESSUM

Verlag WEKA Business Media AG
Hermetschloostrasse 77
CH-8048 Zürich
www.weka.ch

Herausgeber Stephan Bernhard

Redaktion Marco S. Meier

Korrektorat Margit Bachfischer M.A., Bobingen

Layout/Satz Tonio Schelker

Publikation 10 × jährlich, Abonnement: CHF 98.– pro Jahr, Preise exkl. MWST und Versandkosten.
Als digitale Publikation erhältlich unter: www.weka-library.ch

Bildrechte www.istockphoto.com

Bestell-Nr. 9231